Université Mohammed Premier
Faculté des Sciences
Département de Mathématiques

Le laboratoire ACSA organise

Ses deuxièmes journées :

Algèbre, Théorie des Nombres et Leurs Applications

LIVRE DES RÉSUMÉS

24 - 25 Novembre 2017.

Contents

Invited Speakers **4**

B. ALLOMBERT. Institut de Mathématiques de Bordeaux
Aspects combinatoires et algorithmiques des fonctions L d'Artin **4**

T. KOMATSU. School of Mathematics and Statistics Wuhan, China
Several identities of generalized Stirling numbers and degenerate Bernoulli polynomials and poly-Cauchy polynomials **5**

Abstracts **5**

S. ABDELALIM. Faculty of Sciences Ain Chock of Casablanca
On Gneralized Hopfian Abelian Group in the Category of Algebraically Compact Abelian Group **6**

M. A. AMRI. Faculty of Sciences of Oujda
On the Sato-Tate conjecture **7**

S. AOUISSI. Faculty of Sciences of Oujda
Subfields of the 3-Hilbert class field of $\mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ **8**

K. BELHROUKIA. Université Ibn Tofail, Laboratoiare AMGNCA, Kénitra
Dèveloppement en fractions continues de l'opèrateur de Heinz **9**

J. BENAMARA. Faculté des Sciences, Oujda
Idéaux réduits d'un corps cubique pur cas monogène **10**

I-E. BENKOUDAD. Mouhammed First University - Oujda
Rhythms of Arabic words and Fibonacci words **11**

O. BOUGHALEB. Mohamed Ben Abdellah University, FSDM, Fez
On the normality of a monogenic algebra **12**

A. CHILLALI. Mohamed Ben Abdellah University, FP, LSI, Taza
RSA trapdoor **13**

Y. DOUZI. Faculty of Sciences of Oujda
Classification automatique des textures par les Réseaux de Neurones Artificiels **14**

H. EL ALAOUI. Faculty of Sciences Dhar Al Mahraz, Laboratory of geometric and arithmetic algebra, Fez
On P-2-Bézout Rings **15**

M. EL GARN. Faculty of Sciences Ain Chock of Casablanca
Characterization of the Automorphisms of any Free Cyclic Module over Integral Factorial having the Extension Property **16**

M. ES-SAIDI. Moulay Ismail university. Faculty of Sciences, Meknes
Nil-clean property in amalgamated algebras along an ideal **17**

S. EZZIRI. University Hassan II of Casablanca, FSTM
Variant of Schnorr zero-knowledge protocol **18**

M. HAYNOU. Faculty of Sciences and Technology, Errachidia
On the rank of the 2-class group of pure quartic number field $\mathbb{Q}(\sqrt[4]{pd^2})$ where $p \equiv 5 \pmod 8$ **19**

J. HLAL. CRMEF, ANO Laboratory, Oujda
Characterization of Extrema of a Pseudoconvex Functions in Terms of Proximal Subdifferential **20**

I. JERRARI. Faculty of Sciences of Oujda
Capitulation of the 2-ideal classes of K=k$\left(\sqrt{-p\varepsilon\sqrt{l}}\right)$ of type $(2,\ 2,\ 2)$ **21**

M. KACHAD. Faculty of Sciences and Technology of Errachidia
On Drazin-Ruston elements of a Banach algebra **22**

K. DRISS. Faculty of Sciences and Techniques of Mohammedia
A note on finite products of fields **23**

E. H. LAAJI. Faculty of Sciences of Oujda
Lattice Based Cryptography **24**

Y. MAZIGH. Faculty of Sciences of Meknes
On Iwasawa theory of Rubin-Stark units and narrow class groups **25**

M. OULD SAID. Université Cheikh Anta Diop de Dakar
Crypto Système à Clé Publique de McEliece basé sur les Produits Codes matrices **26**

M. REZZOUGUI. Faculté des Sciences-Oujda
Sur la $\mathbb{Z}_2$-extension cyclotomique de certains corps quadratiques réels **27**

M. SABIRI. Faculty of Sciences and Technology of Errachidia
Quasi-Cyclic Codes **28**

T. SERRAJ. Faculty of Sciences of Oujda
How to generate secure elliptic curves for efficient cryptographic applications **29**

M. SOUHAIL. Faculty of sciences Ain Chock of Casablanca
Electronic voting on elliptic curves and security **30**

K. SOUILAH. Faculty of Sciences of Oujda
Some characterizations of Jordan homomorphisms on Banach algebras **31**

M. Tamimi. Faculty of Sciences of Oujda
Introduction sur les corps quartiques cycliques réels **32**

Aspects combinatoires et algorithmiques des fonctions L d'Artin

Bill ALLOMBERT

Institut de Mathématiques de Bordeaux
Université de Bordeaux
France
Bill.Allombert@math.u-bordeaux.fr

Les fonctions L d'Artin sont des objets centraux en théorie algébriques des nombres qui peuvent servir à l'étude des extensions non-abéliennes des corps de nombres et sont l'objet du programme de Langlands.

Nous avons implanté dans le système de calcul formel PARI/GP des algorithmes permettant le calcul des coefficients et des valeurs numériques des fonctions zeta de Dedekind, et des fonctions L de Hecke et d'Artin.

En première partie nous rappelons les définitions et les propriétés et conjectures sur les fonctions L d'Artin.

En seconde partie, nous montrons comment le théorème de Brauer et les propriétés de fonctorialité des fonctions L d'Artin peuvent être utilisés pour accélérer les algorithmes de calculs.

Pour conclure, nous montrons comment ces algorithmes permettent de donner des exemples numériques pour le théorème de Langlands-Tunnel et la correspondance de Deligne-Serre avec les formes modulaires de poids 1, que nous pouvons calculer grace à un programme dû à Henri Cohen et Karim Belabas qui est disponible dans PARI/GP.

Références

[1] The PARI Group, *PARI/GP version 2.10*, 2017 Bordeaux
`http://pari.math.u-bordeaux.fr`

[2] Henri Cohen, Fredrik Strömberg, *Modular form : a classical approach*
`http://bookstore.ams.org/gsm-179`.

[3] Pierre Deligne, Jean-Pierre Serre, *Formes modulaires de poids 1*, Annales scientifiques de l'É.N.S. 4e série , tome 7, no 4 (1974), p. 507-530
`https://publications.ias.edu/sites/default/files/Number24.pdf`.

[4] Prasad, Dipendra ; Yogananda, C. S. (2000), Bambah, R. P. ; Dumir, V. C. ; Hans-Gill, R. J., eds., *A* Report on Artin's Holomorphy Conjecture, Birkhäuser Basel, pp. 301-314.
`http://www.math.tifr.res.in/~dprasad/artin.pdf`.

Several identities of generalized Stirling numbers and degenerate Bernoulli polynomials and poly-Cauchy polynomials

Takao KOMATSU

School of Mathematics and Statistics Wuhan
University Wuhan 430072 P. R. China
tkomatsu31@msn.com

As generalizations of one simple formula for Harmonic numbers, we give several identities of generalized Stirling numbers and degenerate Bernoulli polynomials. We present some expressions of values at nonnegative integers of poly-Cauchy polynomials as finite sums involving Stirling numbers. We also give expressions of Stirling numbers as finite sums involving values of poly-Cauchy polynomials, as well as generating series for values of poly-Cauchy polynomials at nonnegative integers.

References

[1] L. C. Hsu and P. Shiue, A unified approach to generalized Stirling numbers, Adv. in Appl. Math. **20** (1998), 366–384.

[2] K. Kamano and T. Komatsu, Poly-Cauchy polynomials, Mosc. J. Comb. Number Theory **3** (2013), 183–209.

On Gneralized Hopfian Abelian Group in the Category of Algebraically Compact Abelian Group

Seddik ABDELALIM

Laboratory of Topology Algebra, Geometry and Discrete Mathematics.
Department of Mathematical and Computer Sciences,
Faculty of Sciences Ain Chock, Hassan II University of Casablanca
Morocco
seddikabd@hotmail.com

An abelian group A is called Hopfian if for any surjective endomorphism f of A then f is an automorphism of A . In this paper We will characterize the Gneralized Hopfian abelian group in the category of Algebraically Compact abelian group. We know that the p-component of Gneralized Hopfian torsion abelian group is also Gneralized Hopfian. After we construct a Gneralized Hopfian abelian group but its the p-component of A isn't Gneralized Hopfian abelian group.

References

[1] Seddik. Abdelalim *Characterization The strongly Co-Hopfian abelian groups in the Category of Abelian torsion Groups* Journal of Mathematical analysis Volume 6 ISSUE 4(2015), PAGES 1-10.

[2] S. Abdelalim and H. Essannouni, *Characterization of the Inessential Endomorphisms in the Category of Abelian Groups.* Pub. Mat. 47 (2003) 359-372. 659-672

[3] A. Haghany and M.R. Vedadi, *Generalized Hopfian Mdules,* Journal of Algebra (2002), p 324-341.

[4] V.A Hiremath, *Hop en Rings and Hop en Modules,* Indian J. pure appl. Math. 17(7),(1986) 895-900

[5] A. Hmaimou, A. Kaidi and E. Sanchez Campos, *Generalized Fitting modules and rings,* Journal of Algebra 308 (1) (2007), 199-214.

[6] A. kaidi et M. Sangharé,*Une caractérisation des anneaux artiniens à ideaux principaux,* Lecture notes in Mathématique 1328 (1988) 245-254.

[7] G. Baumslag, *Hopficity and abelian groups, Topics in Abelian groups.* Ed.by J.Jrwin and E. A. Walker, scott foresman and company,1963,331-335.

[8] R.A. Beaumont, *Groups with isomorphic proper subgroups.* Bull Amer. Math. Soc,51(1945)381-387.

[9] R. Bear *Groups without proper Isomorphic Quotient groups.* Bull Amer. Math. Soc,50 (1944) 267-278.

[10] P. Crawley, *An Infinite Primary Abelian Groups Without Proper Isomorphic Subgroups.* Bull. Amer. Math Soc.68 (1962) 462-467.

[11] L. Fuchs, *Infinite Abelian Groups,* vol. 1,2 Academic press New York, 1970.

On the Sato-Tate conjecture

Mohammed Amin AMRI

ACSA Laboratory, Department of Mathematics, Faculty of Sciences, Mohammed First University, Oujda, Morocco.
m1.amri@ump.ac.ma

Joint work with: M'hammed ZIANE

The recent proof of the Sato-Tate Conjecture is one of the breakthrough results in mathematics recently by Barnet-Lamb, Geraghty, Harris, Shepherd-Barron and Taylor. The Sato-Tate Conjecture is a statement about the statistical distribution of certain sequences of numbers. Let $k \geq 2$ and $f = \sum_{n\geq 1} a(n)q^n$ be a normalised cuspidal Hecke eigenform of weight $2k$ for $\Gamma_0(N)$ without complex multiplication. Then the Sato-Tate Conjecture says that the numbers $\frac{a(p)}{2p^{(k-1)/2}}$ are equidistributed in $[-1, 1]$ with respect to a certain measure when p runs through the primes not dividing N. By Modularity Theorem, it is also possible to state the conjecture for elliptic curves. Therefore, we can state the conjecture in terms of Frobenius angles. In this case, the Sato-Tate Conjecture tells these angles are distributed according to the function where is the Frobenius angle with . In this talk, we will consider the Sato-Tate Conjecture for modular forms with its history and consequences.

References

[1] Amri, M. A., Ziane, M .: Angular changes of complex Fourier coefficients of cusp forms. arXiv preprint arXiv:1704.00982v4 (2017)

[2] Barnet-Lamb, Geraghty, D., Harris, M., Taylor, R .: A Family of Calabi-Yau Varities and Potential Automorphy II, *Pub. Res. Inst. Math. Sci.*, **47**, (2011), 29-98,

[3] Shimura, G.: On Modular Forms of Half-Integral Weight, *Annals of Math.*, **97**, (1973), 440-481.

[4] Niwa, S .: Modular forms of half integral weight and the integral of certain theta-functions. Nagoya Mathematical Journal,**56**, (1975),147-161.

Subfields of the 3-Hilbert class field of $\mathbb{Q}(\sqrt[3]{p}, \zeta_3)$

Siham AOUISSI

ACSA Laboratory, Department of Mathematics and Computer Sciences,
FSO, Mohamed 1st University,
Oujda - Morocco.
aouissi.siham@gmail.com

Joint work with: Moulay Chrif ISMAILI and Mohamed TALBI

Let $\mathrm{k} = \mathbb{Q}(\sqrt[3]{p}, \zeta_3)$ the normal closure of the pure cubic field $\mathbb{Q}\left(\sqrt[3]{p}\right)$, where p is a prime number such that $p \equiv 1(mod\ 9)$, and let $\mathrm{k}_3^{(1)}$ be the 3-Hilbert class field of k. The 3-component of the class group of k is isomorphic to $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. By the aid of class field theory, we determine all unramified sub-extensions of $\mathrm{k}_3^{(1)}/\mathrm{k}$.

References

[1] P. Barrucand and H. Cohn, *Remarks on principal factors in a relative cubic field*, *J. Number Theory* **3** (1971), 226–239.

[2] R. Dedekind, *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern.* J. für reine und angewandte Mathematik, Bd. **121** (1900), 40-123.

[3] F. Gerth III, On $3-$class groups of certain pure cubic fields, *Bul. Austral. Math. Soc.*, Vol. **72** (2005), 471–476.

[4] T. Honda, *Pure cubic Fields whose Class Numbers are Multiples of Three*, *J.Number Theory* **3** (1971), 7–12.

[5] The PARI Group, PARI/GP, Version 2.3.4, Bordeaux, 2008, `(http://pari.math.u-bordeaux.fr)`.

[6] M.C. Ismaili, *Sur la capitulation des 3-classes d'idéaux de la clôture normale d'un corps cubique pur.* Thèse de doctorat, Univ. Laval, Québec. (1992).

Dèveloppement en fractions continues de l'opèrateur de Heinz

Kacem BELHROUKIA

Département de Mathématiques
Université Ibn Tofail, Laboratoiare AMGNCA
Kénitra 14000, Maroc
belhroukia.pc@gmail.com

Joint work with: Ali KACHA and Salah SALHI

Soient A et B deux matrices définies positives, α un nombre réel tel que $0 \leq \alpha \leq 1$. L'opérateur de Heinz de A et B est définie par:

$$H_\alpha(A,B) = A^{\frac{1}{2}} \cdot \frac{\left(A^{-\frac{1}{2}}BA^{-\frac{1}{2}}\right)^{\alpha} + \left(A^{-\frac{1}{2}}BA^{-\frac{1}{2}}\right)^{1-\alpha}}{2} \cdot A^{\frac{1}{2}} \quad 0 < \alpha < 1.$$

Le calcul direct de cet opérateur s'avère difficile par l'apparition des exposants rationnels de matrices.

La motivation principale de ce travail est de déppasser ces diffécultés et de présenter une métode pratique et efficiente pour ce calcul en utilisant les fractions continues matricielles.

Références

[1] T. L. HAYDEN, Continued fractions in Banach spaces, Rocky Mtn. J.Math., 4 (1974), pp. 367-369.

[2] A.N, Khovanski, The applications of continued fractions and their Generalisation to problemes in approximation theory,1963, Noordhoff, Groningen, The Netherlands (chap2).

[3] L. LORENTZEN, H. WADELAND, Continued fractions with applications, Elsevier Science Publishers, 1992.

[4] Gerard J. MURPHY, C^*-Algebras and operators theory, Chapter 2, (1990), Academic press, INC Harcourt Brace Jovanovich, publishers.

[5] G. NETLLER, On trenscendental numbers whose sum, difference, quotient and product are transcendental numbers, Math. Student 41, No. 4(1973), 339-348.

[6] M. RAISSOULI, A. KACHA, Convergence for matrix continued fractions, Linear Algebra and its applications 320 (2000) pp. 115-129.

Idéaux réduits d'un corps cubique pur cas monogène

Jamal BENAMARA

benamarajamal@hotmail.fr

Soit $K = \mathbb{Q}(\sqrt[3]{m})$ Un corps cubique pur, où m est un entier sans facteur cubique et et soit α une racine cubique de m appartenant à K. si $m \not\equiv \pm 1 \pmod 9$, on dit que K est de première espèce, si en outre m est sans facteur carrée, alors l'anneau des entiers de K est $O_K = [1, \alpha, \alpha^2]$. Dans ce papier nous allons déterminer les idéaux réduits d'un tel corps.

Références

[1] **I. Kiming**, *Arithmetic in Pure Cubic Filds After Dedekind.* Department of Mathematics, University of Copenhagen, Universitetsparken 5, DK-2100 Copenhagen, Denmark.

[2] **H. COHEN**, *A course in computational algebraic number theory.* third ed, Springer-Verlag, 1996.

[3] **S. Alaca and K.S. Williams**, *Introductory algebraic number theory.* Cambridge University Press, Cambridge, UK, 2004. .

[4] **G. Tony Jacobs**, *Reduced ideals and periodc sequences in pure cubic fields*, UNIVERSITY OF NORTH TEXAS August 2015.

[5] **C. Prabpayak**, *Orders in pure cubic number fields*, PhD thesis, Univ. Graz. Grazer Math. Ber. 361, 2014, iii+84pp.

[6] **H.C. Williams and D. Shanks**, *A note on class-number one in pure cubic fields*, Mathematics of Computation 33 (1979), no. 148, 1317-1320.

Rhythms of Arabic words and Fibonacci words

Imad-Eddine BENKOUDAD

Mouhammed First University - Oujda - Morocco
i.benkoudad@ump.ac.ma

Joint work with: Abdelmalek AZIZI - Mouhammed EL AMRANI

The rhythms of Arabic words, as they were studied by *Al Khalil Al Farahidi* (اَلخليل الفرَاهدي), are the sequences of movement (حركة) and silence (سكون), which take into account only the letters uttered in a word.
Al Khalil considers the letter (حرف) and its movement (حركة) as a single phonetic unit. This definition is different from that using consonant and vowel.
The study of the Arabic metric (علم العروض) allowed us to identify the rhythms of Arabic words and, subsequently, the rhythms of speech. We will demonstrate that these rhythms are variants of Fibonacci words.

References

[1] د. مكي درَار [اَلحروف العربية و تبدلَاتهَا الصوتية] (دمشق) .من سلسلة اللّسَانيَات, 2007.

[2] Fibonacci cube and Fibonacci words,
https://en.wikipedia.org/wiki/Fibonacci_cube
Helianthe Caure : Canons rythmiques et pavages modulaires,
https://tel.archives-ouvertes.fr/tel-01338353v2/document

On the normality of a monogenic algebra

Omar BOUGHALEB

Mohamed Ben Abdellah University, FSDM, Fez , Morocco
boughaleb.01omar@gmail.com

Joint work with: Mohammed CHARKANI ELHASSANI

Let $(R, \pi R, k)$ a discrete valuation ring, $\mathfrak{p} = \pi R$ the prime ideal of R, and k its residue field. Let K the quotient field of R, L a finite extention of K, O_L the integral closure of R in L, $\alpha \in O_L$ a primitive element of L, $P = Irr(\alpha, K) \in R[X]$. the purpose of this paper is to construct a ring that contains $R[X]/(P)$ and contained in O_L in the case where P does not satisfy the Dedekind criterion, that is to say that the R-algebra $R[x]/(P)$ is not normal.

References

[1] M. F. ATIYAH and I. G. MACDONALD, *Introduction to commutative algebra* , ADDISON-WESLEY COMPANY, (1969).

[2] N. BOURBAKI, *Algèbre chapitre: 1 à 5*, 1981, Masson.

[3] Cohen, H *A Course in Computational Algebraic Number Theory. Berlin, Springer.*,(1995).

[4] Hallouin, E, *Calcul de fermeture intégrale en dimension 1 et factorisation.*, Thèse de doctorat de l'Universite de Poitiers (1998).

RSA trapdoor

Abdelhakim CHILLALI

Sidi Mohamed Ben Abdellah university, FP, LSI, Taza, Morocco
abdelhakim.chillali@usmba.ac.ma

We could factor a RSA number of 33403 size, in a time of $1367,942$ second. A twin prime is a prime number that has a prime gap of two, in other words, differs from another prime number by two, for example the twin prime pair $(5,3)$. In this work we define a new notion: "r-prime number of degree k" and we give a new RSA trap-door one-way. This notion generalized a twin prime numbers because the twin prime numbers are 2-prime numbers of degree 1.

References

[1] Rivest, R.; Shamir, A.; Adleman, L. (February 1978). *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*. Communications of the ACM 21 (2): 120?126. doi:10.1145/359340.359342.

[2] Robinson, Sara (June 2003). *Still Guarding Secrets after Years of Attacks, RSA Earns Accolades for its Founders*. SIAM News 36 (5).

[3] Boneh, Dan (1999). *Twenty Years of attacks on the RSA Cryptosystem*. Notices of the American Mathematical Society 46 (2): 203?213.

Classification automatique des textures par les Réseaux de Neurones Artificiels

Youssef DOUZI

Mohammed First University, Faculty of Sciences, Laboratory ACSA,
Oujda,
Morocco
douzi.ysf21@gmail.com

Mohamed BENABDELLAH et Abdelmalek AZIZI

La texture joue un rôle très important dans l'identification et l'extraction des informations thématiques contenues dans l'image. L'analyse des textures est un vaste champ dont l'objectif est d'identifier la nature d'une texture, soit via des algorithmes de classification, soit via des algorithmes synthétiques visant à la création d'une texture, visuellement similaire à la texture d'origine.

Notre objectif est de faire une reconnaissance des différents types de tumeurs en travaillant sur des images médicales et de décrire une nouvelle approche de la reconnaissance automatique des textures dans les images numériques en utilisant des réseaux de neurones artificiels [RNA]. Pour cette raison, on a essayé dans un premier temps de tester sur la base de données Brodazt.

Références

[1] Amroun Fazia, *extraction de la composante texture d'une image*, mars 2013.

[2] A. P. pentland, *Fractal based description of natural*, scenes.IEEE Trans.on PAMI ;Vol,6,N6,pp,661-674,1984.

[3] D.R Mitchelle,C.R. Myers et W.Boyne.A max-min measure for image texture analysis,IEE Trans.on computer Vision,pp,408-414,1977

[4] El Moustafa Daoudi, El Miloud Jaara, and Nait Cherif, *Parallelization of Image Compression on DistributedMemory Architecture*, 8th International Conference, HPCN Europe 2000 Proccedings, The Netherlands, May 2000.

[5] F. G. peet et T. S. Sahota, *Surface curvature as a measure of image texture*, IEEE Tans.on PAMI,Vol.7,N6,pp.734-738,1985.

[6] G.Brown,G.Michon et J.Peyriere, *On the multifractal analysis of measures*, In Journal of stat ;Phys.t.66,pp.775-790,1992.

[7] G.M.Haley et B.S Manjunath, *Rotation-invariant texture classification using modified gabor filters*, In ICP95,Washington,pp,262-265,September 1995.

[8] Hajji Tarik, Jaara Elmiloud, *Digital Movements Images Restoring by Artificial Neural Networks*, Computer Science and Engineering p-ISSN : 2163-1484 e-ISSN : 2163-1492 2014 ; 4(2) : 36 42 doi :10.5923/j.computer.20140402.02.

[9] Hajji Tarik, Jaara Elmiloud, *Signing Digital Images by Artificial Neural Networks* International journal ofmathematics and computation ISSN 0974-5718 (Print) ; ISSN 0974-570X-2014.

[10] J. Fridrich, *Methods for detecting changes in digital images*, Proceedings IEEE Int. Conf. on Image Processing (ICIP'98),Chicago, USA, Oct. 1998.

On P-2-Bézout Rings

Haitham EL ALAOUI

Sidi Mohamed Ben Abdellah University
Faculty of Sciences Dhar Al Mahraz, Laboratory of geometric and arithmetic algebra, Fez
Morocco
elalaoui.haithame@gmail.com

Joint work with: Hakima MOUANIS

In this paper, we introduce a generalization of the well-known notion of a "P-Bézout" ring and a "2-Bézout" ring, which we call a "P-2-Bézout" ring. We establish the transfer of this notion and the notion of "2-Bézout" ring to trivial ring extensions. We conclude with a brief discussion of the scope and limits of our results.

References

[1] S. Glas, *Commutative Coherent rings*, Lecture Notes in Mathematics, 1371, Springer-Verlag, Berlin, 1989.

[2] H.Huckaba, *Commutative rings with zero divisors*, Marcel Dekker, New York, 1988.

[3] J. J. Rotman, *An Introduction to Homological Algebra*, Academic Press, New York, 1979.

Characterization of the Automorphisms of any Free Cyclic Module over Integral Factorial having the Extension Property

Mostafa EL GARN

Laboratory of Topology Algebra, Geometry and Discrete Mathematics.
Department of Mathematical and Computer Sciences,
Faculty of Sciences Ain Chock, Hassan II University of Casablanca, Morocco
elgarnmostafa@gmail.com

Joint work with: Seddik. ABDELALIM, Abdelhak CHAICHAA

Let A be an integral factorial ring, if M is a module over A and $\alpha \in Aut_A(M)$. We say that α satisfies the Extension Property, if pour tout monomorphism $\sigma : M \longrightarrow N$ there existe $\widehat{\alpha}$ such that the following diagram

$$\begin{array}{ccc} M & \xrightarrow{\sigma} & N \\ \alpha \downarrow & & \downarrow \widehat{\alpha} \\ M & \xrightarrow{\sigma} & N \end{array}$$

We will show that every automorphism of divisible satisfies the Extension Property, but this result isn't true in general case. After we will give some properties of the automorphisms having the Extension Property. Finally we will Characterize the automorphism of Free Cyclic Module having the Extension Property

References

[1] S. Abdelalim et H. Essannouni, *Characterization of the automorphisms of an Abelian group having the extension property.* Vol. 59, Portugaliae Mathematica. Nova Série 59.3 (2002): 325-333.

[2] S. Abdelalim and H. Essannouni, *Characterization of the Inessential Endomorphisms in the Category of Abelian Groups.* Pub. Mat. 47 (2003) 359-372.

[3] S. Abdelalim and H. Essannouni, *Charcterization of the automorphisms having the lifting property in the Category of abelian Groups.* International Journal Mathematics and Mathematical Sciences 71, p 4511-4516 Hindawai Publishing Corps USA. 2003

[4] L.Ben Yakoub: *Sur un Théorème de Schupp*. Portugaliae. Math. Vol 51 Fasc. 2 (1994)

[5] L.Ben Yakoub et M.P. Malliavin: *Caractérisation des Dérivation Intérieures de l'Algébre de Weyl et de l'Algébre d'Heisenberg Quantique*. Comm. Alg. 24 (1996) N 10, 3131-3148.

[6] M.Dugas and R.Gobel: *Outer Automorphisme of Groups*. Illinois of Math. V 35, N 1 (1991)

[7] L.Fuchs: *Infinite Abelian Groups*. vol. 1 Academic press New York (1970)

[8] M.R.Pettet. *On Inner Automorphisms of Finite Groups*.
Proceeding of A.M.S. V 106, N 1, (1989)

[9] P.E Schupp. *A Characterizing of Inner Automorphisms*
Proc of A.M.S V 101, N 2 . 226-228 (1987)

Nil-clean property in amalgamated algebras along an ideal

Mohammed ES-SAIDI

Moulay Ismail university. Faculty of Sciences
Marjane 2, BP 298, Meknes 50000
Morocco
Saidi1972@gmail.com

Joint work with: Chahrazade BAKKARI

Let $f : A \longrightarrow B$ be a ring homomorphism and let J be an ideal of B. In this Talk, we give a characterization for the amalgamation of A with B along J with respect to f (denoted $A \bowtie^f J$) (introduced and studied by D'Anna, Finocchiaro, and Fontana in [6] and [7]) to be nil-clean.

References

[01] *D.D. Anderson; Commutative rings, in: Jim Brewer, Sarah Glaz, William Heinzer, Bruce Olberding (Eds.), Multiplicative Ideal Theory in Commutative Algebra: A tribute to the work of Robert Gilmer, Springer, New York, (2006), 1–20.*

[02] *M. B. Boisen and P.B. Sheldon; CPI-extension: Over rings of integral domains with special prime spectrum, Canad. J. Math. 29 (1977), 722–737.*

[03] *P. V. Danchev, W. Wm. McGovern, Commutative weakly nil clean unital rings, Journal of Algebra 425(2015), 410–422.*

[04] *A.J. Diesl, Nil clean rings, J. Algebra 383 (2013), 197–211.*

[05] *J.L. Dorroh; Concerning adjunctions to algebras, Bull. Amer. Math. Soc. 38 (1932), 85–88.*

[06] *M. D'Anna, C. A. Finocchiaro, and M. Fontana; Amalgamated algebras along an ideal, Comm Algebra and Aplications, Walter De Gruyter (2009), 241–252.*

[07] *M. D'Anna, C. A. Finocchiaro, and M. Fontana; Properties of chains of prime ideals in amalgamated algebras along an ideal, J. Pure Appl. Algebra 214 (2010), 1633-1641.*

[08] *M. D'Anna; A construction of Gorenstein rings; J. Algebra 306(2) (2006), 507–519.*

[09] *M. D'Anna and M. Fontana; The amalgamated duplication of a ring along a multiplicative canonical ideal, Ark. Mat. 45(2) (2007), 241–252.*

[10] *M. D'Anna and M. Fontana; An amalgamated duplication of a ring along an ideal: the basic properties, Journal of Algebra and its Applications, 6(3) (2007), 443–459.*

[11] *T. Koşan, Z. Wang, Y. Zhou; Nil-clean and strongly nil-clean rings, Journal of Pure and Applied Algebra 220 (2016), 633–646*

Variant of Schnorr zero-knowledge protocol

Salma EZZIRI

University Hassan II of Casablanca, FSTM
Morocco
Salma.ezziri@gmail.com

Joint work with: Omar KHADIR

Identification is an important issue in public key cryptography. It is used in various situations, such as authorization to access to a server, digital signatures, exchange of communication between a customer and bank. The security of identification protocol is based on difficult mathematical questions, like discrete logarithm, factoring and computing square root modulo a large composite number.
In 1989 Schnorr proposed an identification scheme based on the discrete logarithm problem. In this work we propose an identification protocol inspired by Schnorr scheme. We study its security and complexity.

References

[1] A. Fiat and A. Shamir, How to prove yourself: practical solutions to identification and signature problems. Springer-Verlag, Lecture notes in computer science, No 263, Advances in cryptology, Proceedings of Crypto '86, pp. 186-194, 1987.

[2] L. Guillou and J.-J. Quisquater : A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, Proc. of Euro Crypt '88, Springer Verlag LNCS series.

[3] T. Okamoto, Provably secure and practical identification schemes and corresponding signature schemes. In : Brickell E.F. (eds) Advances in Cryptology Crypto '92. Crypto 1992. Lecture Notes in Computer Science, v.740. Springer, Berlin, Heidelberg.

[4] Schnorr, Efficient identification and signatures for smart cards, in G Brassard, ed. Advances in Cryptology - Crypto '89, pp. 239-252, Springer-Verlag, 1990. Lecture Notes in Computer Science, v.435.

[5] A. Shamir, Identity-based cryptosystems and signatures schemes, Springer-Verlag, Lecture notes in computer science, No 196, Advances in cryptology, Proceedings of Crypto '84, pp. 47-53, 1985.

[6] D. R. Stinson, Cryptography: Theory and practice, third Edition (Discrete mathematics and its applications), 1995, pp. 268-269.

On the rank of the 2-class group of pure quartic number field $\mathbb{Q}(\sqrt[4]{pd^2})$ where $p \equiv 5 \pmod 8$

Mbarek HAYNOU

Moulay Ismail university. Faculty of Sciences and Technology
P.O. Box 509-Boutalamine, 52 000 Errachidia
Morocco.
haynou_mbarek@hotmail.com

Joint work with: Mohammed TAOUS

Let d be positive square-free integers, $p \equiv 5 \pmod 8$ be prime a with $(p, d) = 1$. Our goal is to compute the rank of the 2-class group of pure quartic number field $\mathbb{Q}(\sqrt[4]{pd^2})$ by the ambiguous class formula .

References

[1] M. TAOUS, Capitulation des 2-classes d'idéaux de certains corps $\mathbb{Q}(\sqrt{d}, i)$ de type $(2, 4)$, thèse, Université. Mohammed Premier Faculté des Sciences , Oujda, 2008 .

[2] G. GRAS, Class field theory, from theory to practice, Springer Verlag 2003.

[3] C. CHEVALLEY, Sur la théorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sc. Tokyo, Sect. 1, t. 2, (1933), 365-476.

[4] J . A. HYMO AND C. J. PARRY, On relative integral bases for pure quartic fields, Indian J. Pure Appl. Math., 23, 1992, 359-376.

[5] C. J. PARRY, A genus theory for quartic fields, J. Reine Angew. Math. 314 (1980), 40-71.

[6] C. J. PARRY, Pure quartic number fields whose class numbers are even, J. Reine Angew. Math. 264 (1975), 102-112.

[7] P. SAMUEL , Théorie Algébrique des Nombres, Edition Hermann, Paris, 2003.

Characterization of Extrema of a Pseudoconvex Functions in Terms of Proximal Subdifferential

Jamal HLAL

CRMEF, ANO Laboratory, Oujda
Morocco
jamalhilal77@gmail.com

In this paper, we give necessary and sufficient optimality conditions for a point to be an extremum of a pseudoconvex function over a convex set. Our principal tool is the proximal subdifferential.
Keywords: Nonconvex calculus, pseudoconvex functions, limiting subdifferential, proximal subdifferential, normal cone.

References

[1] D. Aussel : Subdifferential properties of quasiconvex and pseudoconvex functions: A unified Approach, J. Optim. Th. Appl, vol 97 No.1 29-45 (1998).

[2] J. Dutta : Necessary Optimality Conditions and Saddle Points for Approximate Optimization in Banach Spaces. Sociedad de Estadistica e Investigacion Operativa.Vol 13, No.1, pp 127-143, (2005).

[3] Y. Jabri, A. Jaddar : Characterization of continuous pseudoconvex functions' extrema, Annals of University of Craiova, Math. Comp. Sci. Ser. Vol 31, 47-50, (2004).

[4] A. Y. Kruger : Properties of generalized differentials, Siberian Math. J.26, 822-832, (1985).

[5] S. Lahrech, A. Jaddar, J. Hlal, A.Ouahab, A.Mbarki: Characterization of the extrema of a pseudoconvex function in terms of the limiting and the strong limiting subdifferential. International Mathematical Forum. 2, 2007, no. 55, 2711-2718.

[6] O. L. Mangasarian : Pseudoconvex functions, SIAM J. Control, 3, 281-290 (1965).

[7] B. S. Mordukhovich, Nguyen Mau Nam :Exact Calculus for Proximal Subgradients with Applications to Optimization. ESAIM: Proceedings April 2007, Vol.17, 80-95.

Capitulation of the 2-ideal classes of K=k$\left(\sqrt{-p\varepsilon\sqrt{l}}\right)$ of type $(2,\ 2,\ 2)$

Idriss JERRARI

Mohammed First university, Department of Mathematics
Faculty of Sciences, Oujda
Morocco
idriss_math@hotmail.fr

Joint work with: Abdelmalek AZIZI, Abdelkader ZEKHNINI and Mohammed TALBI

Let $p \equiv 3 \pmod 4$ and $l \equiv 5 \pmod 8$ be different primes such that $\left(\frac{p}{l}\right) = 1$ and $\left(\frac{p}{l}\right)_4 = 1$. Put $k = \mathbb{Q}(\sqrt{l})$ and denote by ε its fundamental unit. Let $K = k\left(\sqrt{-p\varepsilon\sqrt{l}}\right)$, $K_2^{(1)}$ be its Hilbert 2-class field and $K_2^{(2)}$ be the Hilbert 2-class field of $K_2^{(1)}$. The 2-class group $\mathbf{C}_{K,2}$ of K is of type $(2,\ 2,\ 2)$. Our goal, in this communication, is to determine the structure of the metabelian Galois group $G = \mathrm{Gal}(K_2^{(2)}/K)$ thus to study the capitulation of the 2-ideal classes of K in all its unramified abelian extensions within $K_2^{(1)}$.

References

[1] A. Azizi, *Unités de certains corps de nombres imaginaires et abéliens sur* $\mathbb{Q}$, Ann. Sci. Math. Québec, **23** (2), 15-21, (1999).

[2] A. Azizi, I. Jerrari, A. Zekhnini and M. Talbi, *On the second 2-class group* $\mathrm{Gal}(K_2^{(2)}/K)$ *of some imaginary quartic cyclic number field* K, J. Number Theory **177** (2017) 562-588.

[3] E. Brown and C. J. Parry, *The 2-class group of certain biquadratic number fields I*, J. Reine Angew. Math. **295** (1977), 61-71.

[4] M. N. Gras, *Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré* 4 *de* $\mathbb{Q}$, Publ. Math. Fac. Sciences de Besancon, Théorie des Nombres (1977-78).

[5] M. Ishida, *The genus fields of algebraic number fields*, Lecture notes in mathematics 555, Springer-Verlag (1976).

[6] P. Kaplan, *Divisibilité par* 8 *du nombre des classes des corps quadratiques dont le* 2*-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan Vol. **25**, No. 4, (1973), 596-608.

[7] F. Lemmermeyer, *On 2-class field towers of some imaginary quadratic number fields*, Abh. Math. Sem. Hamburg **67** (1997), 205-214

[8] F. Lemmermeyer, *Ideal class groups of cyclotomic number fields I*, Acta Arith. LXXII 4 (1995).

[9] F. Lemmermeyer, *Reciprocity laws*, Springer Monographs in Mathematics, Springer-Verlag. Berlin (2000).

On Drazin-Ruston elements of a Banach algebra

Mohammed KACHAD

Moulay Ismail university. Faculty of Sciences and Technology
P.O. Box 509-Boutalamine, 52 000 Errachidia
Morocco
kachad.mohammed@gmail.com

We introduce the class of Drazin-Ruston elements with respect to a homomorphism between two Banach algebras. In this work, we extend some of the Ruston theory by among other things, developing the Ruston and almost Ruston elements, and spectra relative to an arbitrary homomorphism. In addition we provide a number of application and generalize certain well-known results.

References

[1] M. P. Drazin, *Pseudo-inverses in associative rings and semigroups* , Amer. Math. Monthly 65 (1958), 506-514.

[2] R. Harte, *Fredholm theory relative to a Banach algebra homomorphism* , Math. Z. 179 (1982), 431-436.

[3] T. Mouton and H. Raubenheimer, *Fredholm theory relative to two Banach algebra homomorphisms*, Quaest. Math. 14 (1991), 371-382.

[4] V. Muller, *Spectral theory of linear operators and spectral systems in Banach algebras*, Operator Theory, Advances and Applications , Birkhauser Verlag, Basel-Boston-Berlin, (2007).

[5] V. Rakocevic, *Koliha-Drazin invertible operators and commuting Riesz perturbations*, Acta Sci. Math. (Szeged) 68 (2002), 953-963.

A note on finite products of fields

Karim DRISS

University Hassan II Casablanca, Department of Mathematics, Faculty of Sciences and Techniques of Mohammedia,
P. O. Box 146, 20650 Mohammedia,
Morocco
dkarim@ced.uca.ac.ma

Let R be a commutative ring. Suppose that R is zero-dimensional, it would be interesting to check whether R contains a finite product of fields. Recently many papers have studied Artinian subrings of a commutative ring and direct limit of finite product of fields ([4, 5, 6, 8]). Recall that Artinian rings form an important class of zero-dimensional rings. Moreover, an Artinian ring has only finitely many idempotent elements. Essentially, the characterization of the set of Artinian subrings of a commutative ring is known (see [6]). In this talk we are interested in the Artinian overring of pair of rings, that means, we are looking for intermediate Artinian rings between R and T, where R is a subring of a von Neumann regular ring T.

References

[1] Arapovic, M. *Characterizations of the 0–dimensional rings*, Glasnik. Mat. Ser. **1983**, Vol. 18 (*38*), 39–46.

[2] Arapovic, M. *On the embedding of a commutative ring into a 0–dimensional commutative ring*, Glasnik. Mat. Ser. **1983**, Vol. 18 (*38*), 53–59.

[3] Gilmer, R.; Heinzer, W., *Zero-dimensionallity in commutative rings*, Proc. Amer. Math. Soc. 115, 881-893 **1992**

[4] R. Gilmer and W. Heinzer, *Products of commutative rings and zero-dimensionality*, Trans. Amer. Math. soc. 331 **1992**, 662-680.

[5] R. Gilmer and W. Heinzer, *Artinian subrings of a commutative ring*, Trans. Amer. Math. soc. 336 **1993**, 295-310.

[6] L. Izelgue and D. Karim, *On the set of Artinian subrings of a commutative ring*, Int. J. Comm. Rings 2, **2003**, 55 - 62.

[7] P. Maroscia, *Sur les anneaux de dimension zéro*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur. 56 **1974**, 451-459.

[8] A. R. Magid, *Direct limits of finite products of fields*, Zero-dimensional commutative rings, (Knoxville, TN, **1994**, 299-305, Lecture Notes in Pure and Appl. Math., 171 Dekker, NewYork.

Lattice Based Cryptography

El Hassane LAAJI

Mohammed First University. Faculty of Sciences
Oujda
Morocco
e.laaji@ump.ac.ma

Joint work with : Mohammed ELAMRANI

On assiste actuellement à une perpétuelle évolution de l informatique Quantique ; Et la préoccupation du monde de la sécurité est de concevoir des cryptosystèmes capable de résister à des éventuelles attaques de l ordinateur Quantique. La cryptographie " Lattice-Based-Cryptography " ; est jugée capable de résister Ã des telles attaques, et assurera la relève des cryptosystémes classiques comme RSA , ECDH, etc. qui ont atteints leurs limites. Dans cet exposé ; qui représente un Etat d'Art sur la cryptographie basée sur les réseaux euclidiens, on représentera un rappel des bases théoriques, ainsi que quelques problémes sur lesquelles est construite la cryptographie Lattices ; puis on décrira le systéme NTRU qui est considéré comme un pilier de la cryptographie Lattices, Enfin on conclut avec les axes de la recherche sur cette nouvelle méthode de cryptographie.

Références

[1] Article *internet- Voici le nouvel Ordinateur Quantique le plus rapide au monde- par Etienne Tierry-Ayme du 14 fevier 2017.*

[2] *Quantum and Post Quantum Cryptography - Abderrahmane Nitaj- Laboratoire de Mathématiques Nicolas Oresme Universite de Caen, France .*

[3] *Decade of Lattice Cryptography-Chris Peikert February 17-2016 page 3-8.*

[4] *Article-Quatre millions d échanges de clefs par seconde- TancredeLepoint-ENSEEITH .*

[5] *Introduction Mathematique and Cryptography J.Hostein, J. Pipher, and J. H. Silverman, NTRU .*

[6] *The Ajtai Dwork Cryptosystem and Other Cryptosystems Based on Lattices by Michael Hartmann paper 2015 Zurich University.*

[7] Paper : Lecture to LLL Algorithm , par OdedRegev 2004 ;

[8] *Cryptographie Homomorphe par Jean-Christophe DENOUVELLE -2012 ;*

[9] *La cryptographie du futur Abderrahmane Nitaj- Laboratoire de Mathématiques Nicolas Oresme Université de Caen, France .*

On Iwasawa theory of Rubin-Stark units and narrow class groups

Youness MAZIGH

Moulay Ismail university. Faculty of Sciences Meknes
B.P. 11201 Zitoune, Meknes
Morocco
y.mazigh@edu.umi.ac.ma

Let K be a totally real number field of degree r. Let K_∞ denote the cyclotomic $\mathbb{Z}_2$-extension of K and let L_∞ be a finite extension of K_∞, abelian over K. The goal of this talk is to compare the characteristic ideal of the χ-quotient of the projective limit of the narrow class groups to the χ-quotient of the projective limit of the r-th exterior power of totally positive units modulo a subgroup of Rubin-Stark units, for some $\overline{\mathbb{Q}_2}$-irreducible characters χ of $\mathrm{Gal}(L_\infty/K_\infty)$.

References

[AMO] **J. Assim, Y.Mazigh, H.Oukhaba.** *Théorie d'Iwasawa des unités de Stark et groupe de classes.* Int. J. Number Theory 13 (2017), no. 5, 1165-1190.

[Gr 92] **C. Greither.** *Class groups of abelian fields, and the main conjecture.* Ann. Inst. Fourier (Grenoble) 42 (1992), no. 3, 449-499.

[Ka 93] **B. Kahn.** *Descente galoisienne et K_2 des corps de nombres*. K-Theory 7 (1993), 55-100.

[Ma 16] **Y. Mazigh.** *Iwasawa theory of Rubin-Stark units and class groups.* Manuscripta Math. 153 (2017), no. 3-4, 403-430.

[MR 04] **B. Mazur, K.Rubin.** *Kolyvagin systems*. Mem. Amer. Math. Soc., 168(799):viii+96, 2004.

[Ru 96] **K. Rubin.** *A Stark conjecture "over $\mathbb{Z}$" for abelian L-functions with multiple zeros*. Ann. Inst. Fourier (Grenoble), 46(1):33-62, 1996.

[Ru 00] **K. Rubin.** *Euler systems*. Annals of Mathematics Studies, 147. Hermann Weyl Lectures. The Institute for Advanced Study. Princeton University Press, Princeton,

Crypto Système à Clé Publique de McEliece basé sur les Produits Codes matrices

Mohamed OULD SAID

Université Cheikh Anta Diop de Dakar,
BP 5005 Dakar-Fann,
Senegal
ouldsaid@yahoo.fr

Les applications des produits matrice codes ont également une utilisation pratique en théorie des codes, dans la création des produis matrice codes en cryptosystème PMC est un cryptosystème de McEliece basés sur les produis matrice codes PMC, une famille de codes de distance minimale. Dans cette communication, on essaye d'introduire un crypto système à clef publique utilisant des codes correcteurs d'erreurs (c'est un système deux en un). Le système étudié est le crypto système de McEliece utilisant le produit des codes et des matrices.

Nous allons dans cette communication : faire une cryptographie en proposant une amélioration de l'attaque de décodage, précisément celui du décodage par ensemble d'information sur les codes binaires et ternaires.

Finalement on va proposer une application du cryptosystème de Mc.Elièce en proposant une utilisation des : " Matrix-Product Codes ".

Références

Sur la $\mathbb{Z}_2$-extension cyclotomique de certains corps quadratiques réels

Mohammed REZZOUGUI

Univérsité Mohammed Premier,
Faculté des sciences-Oujda
Maroc
morez2100@hotmail.fr

Soient p_1, p_2 et q des premiers différents tels que $p_1 \equiv p_2 \equiv -q \equiv 1 \bmod 4$, et q_1, q_2 et q_3 des premiers différents tels que $q_1 \equiv q_2 \equiv q_3 \equiv -1 \bmod 4$, désignons par $A(\mathbb{k})$, $A(\mathbb{k}')$ et $A(\mathbb{k}_1)$ les 2-groupes de classes respectifs des corps $\mathbb{k} = \mathbb{Q}(\sqrt{d})$, $\mathbb{k}' = \mathbb{Q}(\sqrt{2d})$ et $\mathbb{k}_1 = \mathbb{Q}(\sqrt{2}, \sqrt{d})$, où $d = p_1p_2q$ ou $d = q_1q_2q_3$. Dans ce papier, on s'intéresse à déterminer tous les corps $\mathbb{k}$ tels que $A(\mathbb{k}) \simeq A(\mathbb{k}_1)$ ou $A(\mathbb{k}') \simeq A(\mathbb{k}_1)$.

Références

[1] R. Greenberg, *On the Iwasawa invariants of totally real number fields,* Amer. J. Math. **98** (1976) 263-284.

[2] T. Fukuda, *Remarks on $\mathbb{Z}_p$-extension of number fields,* Proc. Japan Acad. Ser. A **70** (1994) 264-266.

[3] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper,* J. Reine Angew. Math. **171** (1935) 55-60.

[4] A. Azizi et A. Mouhib, *Sur le rang du 2-groupe de classes de $\mathbb{Q}(\sqrt{m}, \sqrt{d})$ où $m = 2$ ou un premier $p \equiv 1 \bmod 4$* . Trans. Amer. Math. Soc. 353, No 7 (2001), 2741-2752.

[5] H. Wada, *On the class number and the unit group of certain algebraic number fields.* Tokyo U, Fac. of. sc. J. Serie I, 13 (1966), 201-209.

[6] E. Benjamin and C. Snyder, *Real quadratic fields with 2-class group of type (2,2),* Math. Scand. **76** (1995), 161-178.

[7] A. Azizi et A. Mouhib, *Capitulation des 2-classes d'idéaux de $\mathbb{Q}(\sqrt{2}, \sqrt{d})$ où d est un entier naturel sans facteurs carrés,* . Acta Arith. **109** (2003) 27-63.

[8] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower,* J. Number Theory **73** (1998), 182-194.

Quasi-Cyclic Codes

Mohammed. SABIRI

Moulay Ismail university. Faculty of Sciences and Technology
P.O. Box 509-Boutalamine, 52 000 Errachidia
Morocco
moh_sabiri@yahoo.fr

Quasi-cyclic codes over a finite commutative ring are viewed as cyclic codes over a noncommutative ring of matrices over a finite commutative ring. The study of these codes permits to generalize some known results about quasi-cyclic codes over a finite fields and to propose a construction of some quasi-cyclic codes.

References

[1] F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Corecting Codes*, Third printing North-Holland Mathematics Library (1981), Volume 16.

[2] Pierre-Louis Cayrel, Christophe Chabot, Abdelkader Necer, *Quasi-cyclic codes as codes over rings of matrices*, *Finite fields and their applications*, 16 (2010) 100-115.

[3] Christophe Chabot, *Reconnaissance de codes, structure des codes quasi-cycliques*, thesis N° 29-2009.

How to generate secure elliptic curves for efficient cryptographic applications

Taoufik SERRAJ

Mohammed First University. Faculty of Sciences
60000 Oujda
Morocco
taoufik.serraj@gmail.com

Joint work with: Abdelmalek AZIZI and Moulay Chrif ISMAILI

Nowadays, elliptic curves are widely used in many cryptographic applications to secure information exchanged or stored in public networks [1, 2]. In practice, generating good elliptic curves in a cryptographic context is a very difficult task. The first curves were standardized by the NIST (in 2000) [3], but new concerns appeared since then.

In this paper, we discuss the mathematical proprieties of elliptic curves over finite fields for cryptographic applications [4], and we propose a generation process of new curves using PARI/GP system [5].

References

[1] BSI, *Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token*, German Federal Office for Information Security, BSI TR-03110 Version 2.21. 2016.

[2] S. Blake-Wilson, N. Bolyard, V. Gupta, C. Hawk, B. Möller, R.U. Bochum, *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*, Internet Engineering Task Force (IETF), RFC 4492. 2006.

[3] E.B. Barker, *Digital Signature Standard (DSS)*, National Institute of Standards and Technology, FIPS PUB 186-4. 2013.

[4] L.C. Washington, *Elliptic Curves: Number Theory and Cryptography*, CRC press, 2008.

[5] PARI Group, *PARI/GP version 2.9.1*, Bordeaux. 2016.

Electronic voting on elliptic curves and security

Mohamed SOUHAIL

Laboratory of Topology Algebra, Geometry and Discrete Mathematics.
Department of Mathematical and computer sciences.
Faculty of sciences Ain Chock Hassan II University of Casablanca.
email : mohamed90souhail@gmail.com

Joint work with: Seddik ABDELALIM and Abdelhak. CHAICHAA.

The elections require large human and financial resources, electronic voting offers a cheaper method, more secure and it is difficult to buy the votes.
In this work we will talk about cryptography on elliptic curves over fields and over ring, as well as these applications to electronic voting, the motivation is to use secure electronic voting systems based on very difficult cryptographic problems.

References

[1] A. Fujioka, T. Okamoto et K. Ohta, *A practical secret voting scheme for large scale elections*, AUSCRYPT '92,(1992).

[2] M.A.Cerverò, V.Mateu, J.M.Miret, F.Sebé et J.Valera *An Elliptic Curve Based Homomorphic Remote Voting System*, RECSI 2014 , Alicante, 2-5 septiembre 2014.

[3] Xun Yi, Russell Paulet et Elisa Bertino *Homomorphic Encryption and Applications*, SpringerBriefs in Computer Science, 2014.

[4] A. CHILALI, S.ABDELALIM. *The Eliptic Curves* $E_{a,b}(\mathbb{F}_p[e_1, e_2, e_3])$ Gulf Journal of Mathematics Vol 3, Issue 2 (2015) 49-53.

[5] M. VIRAT. *Courbe elliptique sur un anneau et applications cryptographiques.* Thèse Docteur en Sciences, Nice-Sophia Antipolis. (2009).

[6] D. MUMFORD, J. FOGARTY, AND F. KIRWAN.*Geometric Invariant Theory* , volume 34 of A Series of Modern Surveys in Mathematics . Springer-Verlag, 3e edition, 1994.

[7] N.M. KATZ AND B.MAZUR. *Arithmetic Moduli of Elliptic Curves*. Number 108 in Annals of Mathematics Studies. Princeton University Press, 1985.

[8] H.LANGE AND W.RUPPERT. *Complete systems of addition laws on abelian varieties*. Invent.Math. 79, 603-610(1985).

Some characterizations of Jordan homomorphisms on Banach algebras

Khalid SOUILAH

Mohammed First university. Faculty of Sciences
Oujda
Morocco
s.khalide@gmail.com

Joint work with: Mourad OUDGHIRI

In this paper, we characterize Jordan homomorphisms on Banach algebras by product preserving conditions of generalized Drazin invertibility. More explicit forms of such maps are given in the context of the algebra of all bounded linear operators on a complex Banach space.

An additive map ϕ between unital Banach algebras is said to be *Jordan homomorphism* if $\phi(a^2) = \phi(a)^2$ for all a, or equivalently $\phi(ab+ba) = \phi(a)\phi(b)+\phi(b)\phi(a)$ for all a, b; and is said to be *unital* if $\phi(1) = 1$.

It is well-known that every unital Jordan homomorphism ϕ between unital Banach algebras preserves strongly invertibility, that is $\phi(a^{-1}) = \phi(a)^{-1}$ for every invertible element a, see [6]. Moreover, a well-known formulation of Hua's theorem from [5] asserts that every bijective additive unital map on a field K preserving strongly invertibility is either an automorphism or an anti-automorphism. This result was later improved in [2] where it was shown that any bijective additive map $\phi : K \to K$ such that $\phi(a)\phi(a^{-1}) = \phi(b)\phi(b^{-1})$ for every non-zero elements $a, b \in K$ is of the form $\phi = \phi(1)\psi$ where $\psi : K \to K$ is either an automorphism or an anti-automorphism and $\phi(1)$ commutes with every element of K. Hua's theorem was later extended to Banach algebras in [1].

In this paper, our aim consists in giving analogue results for generalized Drazin invertibility and group invertibility.

References

[1] N. Boudi and M. Mbekhta, *Additive maps preserving strongly generalized inverses*, J. Operator Theory **64** (2010), p. 117-130.

[2] M. A. Chebotar, W.-F. Ke, P.-H. Lee and L.-S. Shiao, *On Maps Preserving Products*, Canad. Math. Bull. **48** (2005), p. 355-369.

[3] I. N. Herstein, *Jordan homomorphisms*, Trans. Amer. Math. Soc. **81** (1956), p. 331-341.

[4] I. N. Herstein, *On the Lie and Jordan Rings of a Simple Associative Ring*, American Journal of Mathematics **77** (1955), p. 279-285.

[5] L. K. Hua, *On the automorphisms of a sfield*, Proc. Natl. Acad. Sci. USA **35** (1949), p. 386-389.

[6] M. Mbekhta, *A Hua type theorem and linear preserver problems*, Math. Proc. R. Ir. Acad. **109** (2009), p. 109-121.

Introduction sur les corps quartiques cycliques réels

Mohammed TAMIMI

Université Mohammed Premier, Faculté des sciences d'Oujda
Maroc
med.tamimi@gmail.com

L'exposé est une introduction aux corps quartiques cycliques réels. Je vais présenter les caractéristiques et les formes de ces corps pour aboutir à la forme convenable à l'étude de groupe de classes et qui assuré l'existence d'une base integral relative.

Références

[Zink 66-77] Zink O. *Extension cycliques de degré 2^n sur $\mathbb{Q}$*. Séminaire delange-Pisot-Poitou. Théorie des nombres (1966-196), Tome 8, n 2, exp.n 16, 1-12.

[Peterson 80] Edgar H, Perterson B. *Some contributions to the theory of cyclic quartic extensions of the rationals*. Journal of number théory (1980), volume 12, issue 1, 77-83.

[Jian-er 91] Jian-er T. *Quartic normal extensions of the rational field*. J.Austral. Math. Soc. (1991), (Series A) 51 , 473-482.

[Motoda 03] Motoda Y. *Notes on quartic fields*. Rep. Fa. Sci. Engrg Saga. Univ. Math (2003), Volume 32, n 1, 1-19.

[Motoda 08] Motoda Y. *Appendix and corrigenda to "Notes on quartic fields"*. Rep. Fa. Sci. Engrg Saga. Univ. Math (2008), Volume 37, n 1, 1-8.

[Williams 95] Huard J G, Spearman B K, Williams K S. *Integral bases for quartic fields with quadratic subfields*. Journal of number theory (1995), Volume 51, Issue 1, 87-102.

[Williams 88] Spearman B K, Williams K S. *Cyclic quartic fields with relative integral bases over their quadratic subfields*. Proc. Amer. Math. Soc (1988), Volume 103, n 3, 687-694.

[Parry 90] Hymo J A, Parry Ch J. *On relative integral bases for cyclic quartic fields*. Journal of number theory (1990), Volume 34, Issue 2, 189-197.

[Parry 77] Brown E, Parry Ch J. *The 2-class group of certain biquadratic number fields*. Journal fur die reine und angwandte mathematik (1977), Volume 295, 61-71.

[Parry 78] Brown E, Parry Ch J. *The 2-class group of biquadratic fields II*. Pacific J. Math (1977), Volume 78, 11-26.

[Parry 80] Parry Ch J. *A genus theory for quartic fields*. Journal fur die reine und angwandte mathematik (1980), Volume 314, 40-71.